UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/040,770	12/28/2001	Lester J. Chong	10547-0023-999	2129

20991 7590 03/22/2007

THE DIRECTV GROUP INC
PATENT DOCKET ADMINISTRATION RE/R11/A109
P O BOX 956
EL SEGUNDO, CA 90245-0956

EXAMINER	
NEURAUTER, GEORGE C	
ART UNIT	**PAPER NUMBER**
2143	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	03/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/040,770
Filing Date: December 28, 2001
Appellant(s): CHONG ET AL.

Georgeann S. Grunebach, Reg. No. 33,179
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 3 January 2007 appealing from the Office action mailed 23 October 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct. No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2003/0055962 FREUND 03-2003

SonicWall, Inc. "SonicWALL SOHO Internet Security Appliance", document revision A, part # 232-000019-00, November 1999, 140 pages.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the Appellant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the Appellant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-6, 11-12, 14-15, and 17-19 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Application Publication 2003/0055962 to Freund et al.

Regarding claim 1, Freund discloses a method for content filtering, comprising:

receiving a request for content from a client computer, where said request includes a port number assigned to an application program running on said client computer; (paragraph 0147, specifically step 910)

determining that said port number is a predetermined port number associated with the request for content; (paragraph 0148, specifically step 950)

renumbering said request with a new port number; (paragraph 0149, specifically "...the destination port is set...")

transmitting said request with said new port number to a content filtering server ("sandbox server") that is configured to listen for requests on said new port number; (paragraph 0149, specifically "...reroute this packet to the sandbox server...")

obtaining from said content filtering server an indication of whether said content is restricted based on said request and said new port number. (paragraph 0149, specifically the sentence "Using this information...")

Claim 18 is rejected since claim 18 recites a computer program product that contains substantially the same limitations as recited in claim 1.

Regarding claim 2, Freund discloses the method for content filtering of claim 1, wherein said renumbering comprises:

determining a user of said client computer's filtering privilege and changing said request with said new port number based on said filtering privilege. (paragraph 0149)

Regarding claim 3, Freund discloses the method for content filtering of claim 1, wherein said obtaining further comprises receiving said requested content, thereby indicating that said content is not restricted. (paragraph 0149, specifically the paragraph "An alternative approach...")

Regarding claim 4, Freund discloses the method for content filtering of claim 3, further comprising transmitting said content to said client computer. (paragraph 0149, specifically the paragraph "An alternative approach...")

Regarding claim 5, Freund discloses the method for content filtering of claim 1, wherein said obtaining further comprises receiving a notification that said content is blocked. (paragraph 0149, specifically the paragraph "Using this information...")

Regarding claim 6, Freund discloses the method for content filtering of claim 5, further comprising notifying said client computer that said content is blocked. (paragraph 0149, specifically the paragraph "Using this information...")

Regarding claim 11, Freund discloses the method for content filtering of claim 1, further comprising, after said receiving, determining an Internet Protocol (IP) address of said client computer, such that said method for content filtering applies only to a particular client computer. (paragraph 0147)

Regarding claim 12, Freund discloses the method for content filtering of claim 1, wherein said determining further comprises ascertaining that said port number is TCP (Transmission Control Protocol) port 80. (paragraph 0148, specifically step 950)

Regarding claim 14, Freund discloses a content filtering gateway ("router"), comprising:

a Central Processing Unit (CPU); communications circuitry; and input/output ports; and a memory containing an operating system; (paragraph 0074)

a port sniffer; (paragraph 0147, specifically the sentence "In step 910...")

a database of filtering privileges and associated port numbers ("router compliance table"); (paragraph 0149) and filtering procedures comprising:

instructions for receiving a request for content from a client computer, where said request includes a port number assigned to an application program running on said client computer; (paragraph 0147, specifically step 910)

instructions for determining that said port number is a predetermined port number associated with the request for content; (paragraph 0148, specifically step 950)

instructions for renumbering said request with one of said associated port numbers from the database of filtering privileges to form a new port number; (paragraph 0149, specifically "...the destination port is set...")

instructions for transmitting said request with said one of said new port number to a content filtering server that is configured to listen for requests on said new port number; (paragraph 0149, specifically "...reroute this packet to the sandbox server...")

and instructions for obtaining from said content filtering server an indication of whether said content is restricted based on said request and said new port number. (paragraph 0149, specifically the sentence "Using this information...")

Regarding claim 15, Freund discloses the content filtering gateway of claim 14, wherein said memory further comprises a filtering database containing a filtering database of Internet Protocol (IP) addresses and their associated filter privileges. (paragraph 0147)

Regarding claim 17, Freund discloses the content filtering gateway of claim 14, wherein said memory further comprises authentication procedures ("security module"). (paragraph 0147)

Regarding claim 19, Freund discloses a system for content filtering, comprising:

at least one content server that stores content ("Web site"); (paragraph 0007) (see also Figure 3, element 350)

at least one client computer configured to transmit a request for said content to said at least one content server, where said request contains an address of said content server and a port number associated with said request for said content ("destination IP address" and "destination port"); (paragraph 0007 and 0147)

a gateway coupled to said at least one client computer, where said gateway is configured to receive and renumber said request with a new port number associated with a filter privilege of a user of said at least one client computer; (paragraph 0149, specifically "...the destination port is set...")

a content filtering server, configured to block restricted content based on said filter privilege, said request and said new port number ("sandbox server"); (paragraph 0149) and

a switch coupled to said gateway, said content filtering server, and said at least one content server, where said switch is configured to listen for said request on said new port number and to redirect said request to said content filtering server. ("routing component"; Figure 3, element 313)

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a),

the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Appellant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 7-10 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund et al in view of "SonicWall SOHO Internet Security Appliance" ("SonicWall").

Regarding claim 7, Freund discloses the method for content filtering of claim 5.

Freund does not expressly disclose the method further comprising:

receiving login details from said client computer; authenticating a user of said client computer based on said login details; determining said user's filter privileges based on said login details; ascertaining an additional port number based on said filter privileges; renumbering said request with said additional port number; transmitting said request with said additional port number to a content filtering server that is

configured to listen for requests on said additional port number; and acquiring from said content filtering server an indication of whether said content is restricted based on said request and said additional port number, however, Freund does disclose determining said user's filter privileges; ascertaining an additional port number based on said filter privileges; renumbering said request with said additional port number; transmitting said request with said additional port number to a content filtering server that is configured to listen for requests on said additional port number; and acquiring from said content filtering server an indication of whether said content is restricted based on said request and said additional port number as shown above regarding claim 5.

"SonicWall" discloses receiving login details from a client computer; authenticating a user of the client computer based on the login details; and determining a user's filter privileges based on the login details. (pages 99-101, "User Authentication", specifically "Establishing an Authenticated Session")

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of these references since "SonicWall" discloses that authenticating a user and determining a user's filter privileges

based on login details enables a user to bypass the content filter (page 99, "User Authentication", first paragraph). In view of these specific advantages and that the references are directed to using an intermediary device in a content filtering system that determines filtering privileges, one of ordinary skill would have been motivated to combine these references and would have considered them to be analogous to one another based on their related fields of endeavor, which would lead one of ordinary skill to reasonably expect a successful combination of the teachings.

Regarding claim 8, Freund and "SonicWall" disclose the method for content filtering of claim 7.

Freund discloses wherein said acquiring further comprises receiving said requested content indicating that said content is not restricted. (paragraph 0149, specifically the paragraph "An alternative approach...")

Regarding claim 9, Freund and "SonicWall" disclose the method for content filtering of claim 7.

Freund discloses wherein said acquiring further comprises receiving a notification that said content is blocked. (paragraph 0149, specifically the paragraph "Using this information...")

Regarding claim 10, Freund and "SonicWall" disclose the method for content filtering of claim 7.

Freund does not expressly disclose the method further comprising associating said login details with an Internet Protocol (IP) address of said client computer, such that said method for content filtering applies only to a particular client computer, however, Freund does disclose determining an Internet Protocol (IP) address of said client computer, such that said method for content filtering applies only to a particular client computer. (paragraph 0147)

Freund and "SonicWall" do not expressly disclose associating said login details with an Internet Protocol (IP) address of said client computer, such that said method for content filtering applies only to a particular client computer, however, Freund does disclose determining an Internet Protocol (IP) address of said client computer, such that said method for content filtering applies only to a particular client computer. (paragraph 0147). "SonicWall" also discloses wherein the login details are used such that the method for content filtering applies only to a particular client computer (pages 99-101, "User Authentication", subsection "Establishing an Authenticated Session").

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Freund and "SonicWall" since the references suggest that a user uses a client computer that contains an IP address in order to send a request and that the IP address of the client computer is used to filter content (paragraph 0147 of Freund) (page 96, "Source"). In view of these suggestions and teachings shown above, one of ordinary skill would have found it obvious to modify the references so that the login details of the user using the client computer are associated together since, in order for the teachings of "SonicWall" to operate, the user must login from a client computer. The authorized user is bound to a particular client computer at the time of authentication, therefore, one of ordinary skill in the art would recognize that, in order for the user to be authenticated, the user must be associated with a particular client computer.

Regarding claim 16, Freund discloses the content filtering gateway of claim 14.

Freund does not expressly disclose wherein said memory further comprises a user database containing login details for multiple users and each user's associated filter privilege, however, "SonicWall" does disclose this limitation ("user list"; see pages 99-100)

Claim 16 is rejected since the motivations regarding the obviousness of claim 7 also apply to claim 16.

(10) Response to Argument

The Appellant has argued that Freund does not teach or suggest the limitations of the claims. The Examiner respectfully submits that Freund does in fact disclose these limitations as presented for at least the following reasons.

1. The Appellant argues that Freund does not teach or suggest receiving a request for content from a client computer, where said request includes a port number assigned to an application program running on said client computer. First, it is noted that the Appellants readily admit on page 7 of the Appeal Brief that a request for connection to the Internet from a local computer is received by a router (The Examiner has equated the router to be the claimed "content filtering gateway" as described in the claims). The Examiner concurs and, as shown previously by the Examiner in the Final Rejection mailed 26 October 2006, the router or "content filtering gateway" receives such a request from a local or "client" computer.

However, the Appellant argues that "...it is clear that Freund is directed to security issues and not restricting access as set forth in the present claims". The Examiner traverses this argument.

Paragraph 0071 of Freund expressly discloses:

"The present invention involves the delegation of a small portion of the overall operation of the end point security software to a local piece of client premises equipment (such as a router or DSL modem) to enable this separate device to enforce certain basic security rules and procedures. This router-side security component, running on the router or other piece of local client premises equipment, checks to ensure that appropriate end point security software is in place on all of the computers on the LAN. Prior to allowing a local computer to connect to the Internet, the security component on the router verifies that the computer has installed and is running appropriate security software, and is in compliance with other established security policies. If a computer is not in compliance, then the computer's access to the Internet is **restricted** to those activities necessary to get the computer back into compliance. This is accomplished by redirecting the attempted connection by a non-compliant computer to a designated "sandbox" server that can facilitate appropriate corrective action, including the download of appropriate software to correct the non-compliance. The security solution only permits an Internet connection to this sandbox server for the limited purpose of informing the user of the non-compliance and enabling

the user to take the steps necessary to bring his or her computer into compliance. The security solution **limits and denies any other access to the Internet by the non-compliant computer**."

Therefore, in view of the teachings of Freund both here and as previously shown in the Final Rejection, the Examiner submits that this argument is erroneous and that the teachings of Freund are clearly relevant.

Further, the Appellant argues on page 8 of the Appeal Brief that "Paragraph 47 [sp] does not appear to address requesting content." It is assumed that the Appellant is referring to paragraph 0147. However, the Examiner traverses this argument.

Paragraph 0065 of Freund expressly discloses:

"The above-described computer hardware and software are presented for purposes of illustrating the basic underlying desktop and server computer components that may be employed for implementing the present invention. For purposes of discussion, the following description will present examples in which it will be assumed that there exists a "server" (e.g., Web server) that communicates with one or more "clients" (e.g., personal computers running Web browsers such as Netscape Navigator or Microsoft Internet Explorer). The present invention, however, is not limited to any particular environment or device

configuration. In particular, a client/server distinction is not necessary to the invention, but is used to provide a framework for discussion. Instead, the present invention may be implemented in any type of system architecture or processing environment capable of supporting the methodologies of the present invention presented in detail below."

Therefore, in view of these teachings of Freund and as shown previously by the Examiner in the Final Rejection, Freund clearly teaches that the request being sent from a local computer or "client" as admitted by the Appellant and within the context of the disclosures of Freund is a request for content from a client using a Web browser to a server which contains content as reasonably understood by one of ordinary skill in the art in view of these disclosures of Freund concerning a typical client and server system. The Examiner therefore submits that the Appellant's argument in this regard is clearly erroneous.

The Appellant also argues that Freund fails to teach or suggest wherein a port number is assigned to an application program running on the client computer. The Examiner traverses this argument in view of the teachings of Freund and the broadest reasonable interpretation of the claims as required by MPEP 2111.

The Examiner notes that the limitation recites that the port number is "assigned" to an application program running on the client computer. First, the Examiner notes that the claims fail to specifically recite any element within the claims that accomplishes such an assignment. Therefore, the Examiner has reasonably interpreted this limitation in its broadest sense wherein the application program is assigned its well known port number by those of ordinary skill as is well known and used within the art and the disclosures of Freund use this assignment to operate the invention as disclosed.

Paragraph 0027 of Freund discloses:

"HTTP: HTTP is the acronym for "HyperText Transfer Protocol", which is the underlying communication protocol used by the World Wide Web on the Internet. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when a user enters a URL in his or her browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page."

Paragraph 0148 of Freund also discloses:

"In step 950 the routing component determines whether or not the destination port is HTTP (port 80 TCP). If the

destination port is HTTP, then the re-routing manager proceeds in step 951 to manipulate the destination IP address and port."

Therefore, the Examiner submits that the broadest reasonable interpretation of the claim wherein the request includes a port number that is assigned to an application program running on the client computer or a "web browser" as described in Freund that uses the HTTP protocol to request and retrieve content is valid and as is within the knowledge of those of ordinary skill in the art and as also shown in Freund, the port number normally assigned to HTTP is the TCP port number 80. Therefore, it is submitted that at least the disclosures of Freund do in fact anticipate this limitation.

2. The Appellant argues that Freund fails to teach or suggest determining that the port number is a predetermined port number associated with a request for content. The Examiner respectfully traverses this argument.

The Examiner notes that, within the Final Rejection, paragraph 0147 was inadvertently cited for step 950 whereas the paragraph should be paragraph 0148. The Appellant's remark regarding this error is acknowledged.

Paragraph 0148 of Freund discloses regarding step 950, as shown previously:

"In step 950 the routing component determines whether or not the destination port is HTTP (port 80 TCP). If the destination port is HTTP, then the re-routing manager proceeds in step 951 to manipulate the destination IP address and port."

Therefore, Freund expressly discloses that the router or "content filtering gateway" determines whether the port number included with the content request is a predetermined port number associated with the request for content or, in the example shown in Freund, TCP port 80 and the Examiner submits that Freund anticipates this limitation.

3. The Appellant argues that Freund fails to teach or suggest renumbering the request with a new port number and transmitting the request with the new port number to a content filtering server that is configured to listen for requests on said new port number and obtaining from the content filtering server and indication of whether the content is restricted based on the request and the new port number. The Examiner traverses this argument.

First, the Examiner notes that the Appellant admits that the "sandbox server" of Freund, equated with the claimed "content filtering server", listens for a particular port.

Paragraph 0149 of Freund, as shown previously, expressly discloses:

"In step 951 the destination IP address is replaced with the IP address of the sandbox server ("lynksys.zonelabs.com" in this example). Also in step 951, if the entry in the router compliance table is less than 256, then the destination port is set to the value of the table entry plus 8080. For example if the table entry is 1, the destination port is set to port 8081 (which represents 8080 plus 1). This also conveys information to the sandbox server in the HTTP header permitting the sandbox server to categorize the reason for non-compliance. Using this information, the sandbox server then displays a page with information enabling the client to address the specific problem that was detected. An alternative approach that can also be used is to redirect the client to the sandbox server for a warning that he or she was not running the required security software, but then permit the client at his or her option to continue (notwithstanding the warning) and connect to the original destination if he or she elected to do so. Otherwise, in step 951 if the entry is 256 or greater, the destination port is set to port 8080. In this manner, the connection request from a non-compliant client computer is patched and manipulated to reroute this packet to the sandbox server."

Also, paragraph 0095 of Freund discloses:

"When a computer is not compliant, the security solution redirects the user to the sandbox server to inform him or her of the non-compliance. The sandbox server also enables the user to take the steps necessary to bring his or her computer back into compliance. The sandbox server operates by looking for communications on certain port addresses and using the port address as a response code. The different port addresses can, in effect, indicate a certain problem or condition. For example, port 8082 means no client response was received. Other ports can be used to indicate other specific problems."

Paragraph 0078 also discloses:

"In all of these cases, the non-compliant computer 330 is then redirected by the routing component 313 and permitted only a limited Internet connection to sandbox server 360. In this situation, the routing component 313 only allows non-compliant computer 330 to perform a defined set of tasks to address the non-compliance. All other Internet access by computer 330 is disabled."

Paragraph 0040 also discloses:

"One or more computers connect to the Internet through the router. A client-side security module of the present invention is installed on the local computers. In addition, a "sandbox" server is located somewhere on the Internet. Requests to connect

to the Internet from non-compliant computers are redirected to the sandbox server."

Therefore, in view of the disclosures of Freund, the Examiner submits that Freund does in fact anticipate these limitations. Note that, throughout the teachings of Freund, the client must access the content filtering gateway for all Internet communications, therefore, the content filtering gateway must obtain the indication from the content filtering server in order to send the indication to the client.

As shown previously, the Examiner notes for the record that the citation of Freund as cited for the transmitting step discloses a "sandbox server" which has been equated by the Examiner to be a content filtering server as claimed. The Appellant argues on page 8 of the Appeal Brief that "the sandbox server is not a content filtering server" and that "Sandbox server is described as a server that is used to categorize a reason of noncompliance" and "The paragraph also describes the sandbox server as not running required security software". The Examiner submits that these arguments are irrelevant to the issue of whether Freund contains the limitations of the claims since the naming convention of the disclosures of Freund are not relevant. Also, the claims do not specifically require that the "content filtering server" not have any of these features that

are or are not taught within Freund. Therefore, the Examiner submits that these arguments are erroneous.

The Examiner also notes that as noted previously in the Final Rejection, the claims do not specifically recite and therefore require any functional feature other than the claimed "configured to listen for requests on said new port number" and indicating "whether said content is restricted based on said request and said new port number". Limitations from the specification are not read into the claim. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The Appellant asserts on page 8 of the Appeal Brief that the above Examiner's notation in the Final Rejection means that the Examiner do not consider these limitations since the Appellant argues that "these limitations must be considered". The Examiner traverses this assertion since the Appellant has misinterpreted the Examiner's remarks. Since the claim DO NOT recite any other features other than what is claimed, the Examiner is required to ONLY considered the claimed features. To read any other limitations into the claim would violate the Examiner's requirement to interpret the claims in their broadest sense as required by MPEP 2111. As shown previously and above, the Examiner has considered all the limitations of the claims. Since the content filtering server only embodies features as recited

in the claims as shown above and as will be shown, the Examiner submits that the Examiner's correspondence of the "content filtering server" as claimed with the "sandbox server" of Freund is valid.

The Appellant also argues on page 9 of the Appeal Brief that the "sandbox server" "does not listen for communications on a number of ports". However, as shown above in paragraph 0095 and also as shown in paragraph 0117, Freund clearly discloses these limitations.

4. The Appellant argues that Freund does not teach or suggest determining a user of the client computer's filter privilege from a database and changing the request with the new port number based on the filter privilege. However, as shown above and previously in paragraph 0149, Freund clearly discloses this limitation. See also paragraphs 0144 and 0145.

5. The Appellant also argues that Freund does not teach or suggest receiving a notification that the content is blocked. However, as shown above regarding the notification from the content filtering server and as shown previously, Freund clearly discloses this limitation. See also paragraph 0117.

6. The Appellant also argues throughout the Appeal Brief that Freund does not have sort of teaching or suggestion regarding

content filtering. However, as shown above at least in paragraph 0071, Freund clearly discloses such a context.

7. The Appellant also argues that Freund does not teach or suggest authentication procedures. However, such a broad limitation interpreted in its broadest reasonable interpretation can encompass any sort of "authentication procedure". As has been shown above extensively, Freund clearly discloses authentication procedures in the content filtering gateway.

8. The Appellant further argues that the combined teachings of Freund and "SonicWall" fail to teach content filtering. However, as shown above, Freund clearly discloses content filtering. As shown previously, Freund does not expressly disclose a bypass filter as claimed, however, such a bypass filter is disclosed in "SonicWall" and it would have been obvious to combine the teachings of the references for the motivations provided in the Final Rejection. Therefore, the combined teachings of these references teach this limitation.

9. It is submitted that the Examiner's rejections be sustained in view of the teachings of the cited prior art.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

George C. Neurauter, Jr.

Patent Examiner

Art Unit 2143

/gcn/

Conferees:

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

WILLIAM VAUGHN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER